Data Processing Addendum to Agreement

This Data Processing Addendum ("DPA") is supplemental to the PSQuote SAAS Terms and Conditions Agreement and is effective as of the date of the Agreement or any PSQuote Order Form. This DPA provides the terms that apply whenever You or your authorized Affiliates enter Personal Data into PSQuote to be processed in the use of the Services. This DPA only applies to data processed as part of the software Services under the PSQuote SAAS Terms and Conditions Agreement. If CLD Partners or any other affiliate of PSQuote provides implementation, consulting, business analysis, project management, data migration, integration services, or Concierge Support Services under a separate Master Services Agreement, this DPA will not apply to any processing of data that may be part of that work. In that instance, a separate DPA will be entered into between the parties where necessary.

How to Execute this DPA:

This DPA has been pre-signed by PSQuote. To complete this DPA, You must fill in all information in the signature box on page 6 and sign the DPA. Once signed, send the completed DPA to PSQuote at security@psquote.com. Upon PSQuote's receipt of the validly completed DPA at this email address, this DPA will become legally binding.

1. Definitions

Unless the context requires otherwise, capitalized terms in this Agreement shall have the following meanings:

- "Affiliate" means, with respect to any party, any person, partnership, joint venture, corporation, or other entity that directly or indirectly controls, is controlled by, or under common control with such party.
- "Agreement" means the PSQuote SAAS Terms and Conditions to which this Data Processing Addendum is attached.
- "Application" or "Services" means PSQuote.
- "Controller" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data pursuant to Data Protection Laws.
- "Data Protection Laws" means any and all applicable national, international, provincial, federal, state and local laws and regulations relating to data protection, data privacy, data security, or the Processing of Personal Data, including (where applicable) EU Data Protection Legislation, the California Consumer Privacy Act ("CCPA") (California Civil

Code §§ 1798.80, et seq.), and any other provincial or state privacy laws that may take effect during the term of the Agreement.

- "Data Subject" has the same meaning given in the General Data Protection Regulation (GDPR).
- "End User" means each of Your employees, consultants, contractors, partners, representatives, agents, or other individuals who is authorized by You to use the App in accordance with this Agreement and for whom an appropriate Salesforce CRM License has been properly obtained.
- "Personal Data" means any information relating to an identified or identifiable natural person.
- "Processing" has the same meaning given in the GDPR and includes any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "Processor" means an entity which Processes Personal Data on behalf of the Controller.
- "Security Incident" means confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data caused by PSQuote's acts or omissions.
- "Sensitive Data" means (a) racial or ethnic origin; (b) political opinions; (c) religious or philosophical beliefs; (d) trade union membership; (e) genetic data; (f) biometric data for the purpose of uniquely identifying a natural person; (g) data concerning health; (h) data concerning a natural person's sex life; (i) sexual orientation; and (ii) without limiting the foregoing, any additional information that falls within the definition of "special categories of data" under EU Data Protection Legislation or Data Protection Laws.

2. Relationship with Agreement

2.1 Except as amended by this DPA, the Agreement will remain in full force and effect.
2.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control with respect to the subject matter of the DPA.
2.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

General Data Protection Obligations

3. Roles and Responsibilities

3.1 Parties' Roles. With respect to the Processing of Personal Data, You acknowledge and agree that You are a Controller and/or a Processor. You appoint PSQuote, as a Processor. The Parties agree that, for the purposes of the Agreement and this DPA, PSQuote is a "service provider" and You are a "business" consistent with the definitions under the CCPA.
3.2 Processing of Personal Data.

A) Whenever You process Personal Data in Your use of the Services, You will comply with all applicable Data Protection Laws, including by providing notice and obtaining all consents and rights necessary under Data Protection Laws for PSQuote to process Personal Data. For the avoidance of doubt, Your instructions for the Processing of Personal Data shall comply with Data Protection Laws. You shall have sole responsibility for the accuracy, quality, and legality of Personal data which you have acquired and placed or allowed to be placed within your Salesforce environment on the Force.com platform. You specifically acknowledge that Your use of the Services will not violate the rights of any Data Subject.

B) In providing the Services on the Salesforce platform, PSQuote will not, through its Services, remove any of Your Data, including Personal Data, from your environment on the Salesforce platform. PSQuote will treat all of Your Personal Data as Confidential. To the extent that you utilize the Services to process Personal Data, You hereby authorize PSQuote, through its Services, to Process the Personal Data for the purposes described in Exhibit A. The Agreement and this DPA sets out Your complete instructions to PSQuote in relation to the Processing of the Personal Data and any Processing required outside of the scope of these instructions will require prior written agreement between the parties. You acknowledge that PSQuote shall have a right to Process Personal Data in order to provide the Services to You, fulfill its obligations under the Agreement, and for legitimate purposes relating to the operation, support and/or use of the Services such as billing, account management, technical maintenance and support, product development, and sales and marketing. Under no circumstances will PSQuote rent or sell Personal Data.

3.3 Prohibited Data. Unless the Processing of Sensitive Data is otherwise permitted by Data Protection Laws or You obtain PSQuote's prior written consent, You will not provide (or cause to be provided) any Sensitive Data to PSQuote for Processing under the Agreement, and PSQuote will have no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, the obligations of PSQuote under this DPA will not apply to Sensitive Data unless the Processing of Sensitive Data is otherwise permitted by Data Protection Laws or You have obtained PSQuote's prior written consent.

3.4 Description of Processing. A description of the nature and purposes of the Processing, the types of Personal Data, categories of Data Subjects, and the duration of the Processing are set out further in Exhibit A.

3.5 Compliance. You shall be responsible for ensuring that:

(a) You have complied, and will continue to comply, with Data Protection Laws, in Your use of the Services and Your own Processing of Personal Data, including by providing notice and obtaining all consents and rights necessary under Data Protection Laws for PSQuote to process Personal Data; and

(b) You have, and will continue to have, the right to transfer, or provide access to, the Personal Data to PSQuote for Processing in accordance with the terms of the Agreement and this DPA.

4. Data Security

4.1 Security. PSQuote shall implement and maintain appropriate technical and organizational measures designed to protect the Personal Data from accidental or unlawful destruction, loss,

alteration, unauthorized disclosure or access, including as appropriate, the measures referred to in Article 32(1) of the GDPR. Notwithstanding the above, You agree that You are responsible for Your secure use of the Services, including securing Your account authentication credentials, protecting the security of Personal Data when in transit, and taking any appropriate steps to backup Personal Data.

4.2 Security Exhibit. The technical and organizational security measures which PSQuote shall have in place under the Agreement are set out at Exhibit B to this DPA.

5. Additional Security

5.1 Confidentiality of Processing. PSQuote shall ensure that any person engaged in the processing of Personal Data shall be subject to a duty of confidentiality through a written confidentiality agreement and will have received training on their responsibilities under Data Privacy Laws.

5.2 Security Incidents. Upon becoming aware of a Security Incident caused or contributed to by PSQuote or its Services, PSQuote shall notify You without undue delay and shall provide such timely information as You may reasonably require, including to enable You to fulfill any data breach reporting obligations under Data Protection Laws. PSQuote shall take appropriate and commercially reasonable steps to investigate and mitigate the effects of such a Security Incident on the Personal Data under this Agreement. This section 5.2 does not apply to Security Incidents that are caused by You, including Your employees, partners, subcontractors, or agents, or by any third-party that is not controlled by PSQuote.

6. Sub-Processing

6.1 Sub-Processors. You agree that this DPA constitutes Your written authorization for PSQuote to engage Affiliates and third party sub-processors (collectively, "Sub-processors") to Process the Personal Data on PSQuote's behalf. PSQuote will ensure that any sub-processor has agreed to the same obligations as PSQuote does under this agreement. PSQuote will notify you if it will use any Sub-Processor to process Personal Data. You may object, on reasonable grounds, to PSQuote's use of any Sub-Processor and work with PSQuote in good faith to find a commercially responsible alternative solution. If no resolution can be reached, PSQuote will, at its sole discretion, either not appoint such Sub-Processor, or permit You to suspend or terminate the Services in accordance with the termination provisions of the Agreement.

6.2 Sub-processor obligations. Where a Sub-processor is engaged by PSQuote as described in this Section 7, PSQuote shall:

(a) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data Protection Laws; and

(b) remain responsible for any breach of the DPA caused by a Sub-Processor.

7. Cooperation

7.1 Cooperation and Data Subjects' rights. PSQuote shall, taking into account the nature of the Processing, provide commercially reasonable assistance to You insofar as this is possible, to enable You to respond to requests from a Data Subject seeking to exercise their rights under Data Protection Laws in the event You do not have the ability to implement such requests without PSQuote's assistance. In the event that such request is made directly to PSQuote, PSQuote shall, unless prohibited by law, promptly inform You of the same. To the extent legally permitted, You shall be responsible for any costs arising from PSQuote's provision of such assistance.
7.2 Data Protection Impact Assessments. PSQuote shall, to the extent required by EU Data Protection Legislation and at Your sole expense, taking into account the nature of the Processing and the information available to PSQuote, provide You with commercially reasonable assistance with data protection impact assessments or prior consultations with data protection authorities that You are required to carry out under Data Protection Laws.

8. Deletion / Return of Data

8.1 Deletion or return of data: Upon the termination or expiration of the Agreement, upon Your request, provided such request is made within 30 days of the date of termination or expiration of the Agreement, PSQuote will make available any Personal Data that is in PSQuote's possession or control and at the end of that period, PSQuote will, upon Your request, delete or destroy all copies of Personal Data in its possession or control, save to the extent that: (i) PSQuote is required by any applicable law to retain some or all of the Personal Data, (ii) PSQuote is reasonably required to retain some or all of the Personal Data for limited operational and compliance purposes, or (iii) Personal Data has been archived on back-up systems. In all such cases, PSQuote shall maintain the Personal Data securely and limit processing to the purposes that prevent deletion or return of the Personal Data.

9. Authorized Affiliates

9.1. Contractual Relationship. You acknowledge and agree that, by executing the Agreement, You enter into this DPA on behalf of Yourself and, as applicable, in the name and on behalf of Your Authorized Affiliates, thereby establishing a separate DPA between PSQuote and each such Authorized Affiliate subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and is a party only to this DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by You.

SIGNED by the parties or their duly authorized representatives:

Company: _____	Company: PSQuote, LLC
Signature: _____	Signature: DocuSigned by: Joseph P. Lyons
Print Name: _____	Print Name: Joe Lyons
Title: _____	Title: Data Security Officer
Date: _____	Date: 11/11/2025

Exhibit A

Nature and purposes of Processing

PSQuote will process Personal Data only as necessary to perform the Services pursuant to the Agreement and as instructed by You in Your use of the Services.

Categories of Data Subjects

Any categories of individuals whose data You transfer, load, or authorize to be loaded into Your Salesforce.com instance and which You give PSQuote access to.

Categories of data

The Personal Data concerns the following categories of data for the Data Subjects:

- Any Personal Data that You choose to include in Your instance of the Services.

The Personal Data transferred to PSQuote for Processing is determined and controlled by You in Your sole discretion.

Special categories of data (if appropriate)

PSQuote does not intentionally collect or Process any special categories of data in the provision of the Services. You agree not to provide Sensitive Data to PSQuote at any time.

Duration of Processing

The Personal Data will be Processed for the term of the Agreement, or as otherwise required by law or agreed between the parties.

Exhibit B

PSQuote Security Measures

PSQuote will ensure that nothing that is a part of its Services shall operate to transfer your data out of the Force.com platform or Your own environment within that platform. The Salesforce security model which you have agreed to as part of your agreement with Salesforce is adopted and utilized by PSQuote in its Services. In addition, PSQuote will never access or use your data in any way except for the purpose of providing you the Services or to address any technical problems or at Your request with regard to a customer support matter.

In addition to the foregoing, and consistent with the level of access and control that PSQuote may have with regard to any of Your Personal Data, PSQuote has adopted the following technical and organizational security measures:

1. Controls Related to PSQuote Application

(a) PSQuote will maintain documentation on overall application architecture, Process flows, and Salesforce-based security features for applications handling Personal Data.

(b) PSQuote will employ secure programming guidelines and protocols in the development of applications Processing or handling Personal Data.

(c) PSQuote will assess PSQuote security vulnerabilities on a regular basis and with each release cycle and address critical vulnerabilities within a reasonable period of time.

(d) PSQuote will perform code review and maintain documentation of code reviews performed for PSQuote.

(e) PSQuote will employ change management standards for PSQuote.

(f) PSQuote will employ static code analysis tools to evaluate any security vulnerabilities prior to issuing any updates or enhancements to PSQuote.

2. Data-Level Controls

(a) As a Force.com application, encryption of data in transit to or from PSQuote is enforced by the security architecture utilized by the Force.com Platform.

3. End User Computing Level Controls

(a) PSQuote will employ an endpoint security or antivirus solution for end user computing devices that may access customer data.

(b) PSQuote will ensure that end user computing devices that access customer data are encrypted.

(c) PSQuote will ensure that end user access is controlled by, including but not limited to, the following configurations: strong password authentication/multi factor authentication.

(d) PSQuote will implement critical patches on systems that access Personal Data within a reasonable period of time after the patch is identified.

4. Compliance Controls

(a) PSQuote will operate within the parameters of PSQuote's then-current Information Security Policy.

(b) Notwithstanding any of the foregoing, PSQuote will adopt appropriate physical, technical and organizational security measures in accordance with industry standards, including but not limited to, access controls, annual data security training and other employee education, and personnel security measures including performing background checks on all employees.